Положение о мониторинге системы DLP

г. Москва

2020

1. Общие положения

1.1. Положение о мониторинге (далее - Положение) регламентирует процедуру и формы проведения мониторинга с помощью DLP-системы.

1.2. Целью данного Положения является регламентирование обеспечения защиты информации ограниченного доступа, обрабатываемой работниками Компании, с помощью программных (программно-аппаратных) средств, обеспечивающих контроль за использованием технических средств.

1.3. Задачами контроля за использованием технических средств являются:

- фиксация фактов нарушения работниками Компании конфиденциальности защищаемой информации для дальнейшего расследования инцидента и привлечения к ответственности;
- фиксация использования технических средств работниками Компании в личных целях для организации использования технических средств работниками Компании исключительно в целях выполнения трудовых обязанностей и привлечения к ответственности за нецелесообразное использование ресурсов Компании;
- фиксация других неправомерных действий работников для дальнейшего проведения расследования и привлечения к ответственности.

1.4. Настоящее Положение распространяется на контроль за защищаемой Компанией информацией (персональные данные, коммерческая тайна и другие сведения, распространение которых может нанести Компании репутационный или финансовый ущерб), независимо от вида носителя, на котором они зафиксированы.

1.5. Положение о мониторинге, а также дополнения и изменения к нему утверждаются распоряжением начальника отдела-ИБ.

1.6. Настоящее Положение распространяется на работников следующих подразделений Компании:

- Отдел информационных технологий;
- Отдел информационной безопасности.

1.7. В настоящем положении используются следующие термины:

Защищаемая информация – информация, относящаяся к персональным данным, к коммерческой тайне или к другой информации ограниченного доступа.

Коммерческая тайна – режим конфиденциальности информации, позволяющий Компании при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Парольная политика - это набор правил, направленных на повышение безопасности компьютера путем поощрения пользователей к использованию надежных паролей и их правильному использованию.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.8. Принятые сокращения:

ИБ - Информационная безопасность

КТ - Коммерческая тайна

ПДн - Персональные данные

РФ - Российская федерация

ФЗ - Федеральный закон

DLP - Data Leak Prevention (система предотвращения утечек информации)

2. Правовые и нормативно-методические источники

Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27 декабря 2002 года № 184-ФЗ «О техническом регулировании»;
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Гражданский кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации.

3. Правила использования технических средств обработки, хранения и передачи информации

3.1. Работникам Компании разрешено:

- пользоваться техническими устройствами, выданными Компанией и включенными в перечень использования технических устройств;
- посещать доверенные веб-сайты;
- пользоваться рабочей почтой для выполнения должностных обязанностей;
- хранить личную информацию на корпоративных ресурсах (рабочие станции и корпоративные мобильные устройства) и передавать ее по корпоративным каналам связи (корпоративная электронная почта, корпоративные мессенджеры, корпоративные файловые хранилища и т.д.).

3.2. Работникам Компании запрещено:

- посещать с рабочей станции и корпоративных мобильных устройства каких-либо социальных сетей и мессенджеров в личных целях;
- использовать личные съемные устройства (флэшки, диски и т.д.);
- разглашать конфиденциальную информацию компании;
- хранить личную информацию на корпоративных устройствах.

Корпоративные каналы связи и средства обработки информации должны использоваться работниками исключительно для служебных (производственных) целей.

4. Организация контроля использования технических средств хранения, обработки и передачи информации работниками Компании

4.1. Общие сведения

Контроль осуществляется с помощью анализа информации и анализа действий работников.

Обязанность по администрированию системы возлагается на ответственного работника ИБ-отдела. В задачи ответственного работника системы входит анализ событий DLP-системы, оповещение начальства о подозрительных действиях работников Компании и потенциальных инцидентах ИБ.

Дополнительный контроль и верификация инцидентов ИБ осуществляется начальником ИБ-отдела.

Для принятия решения о принимаемых в дальнейшем мерах по устранению инцидента, необходимо определить уровень критичности каждого инцидента ИБ. Если инцидент имеет высокую или среднюю степень критичности, то ответственный работник ИБ-отдела обязан сообщить о нем начальнику ИБ-отдела. Инциденты с низким уровнем критичности дополнительно обрабатываются и на основании данных, полученной от DLP-системы, делается вывод о действительной степени критичности инцидента.

4.1.1. Парольная политика DLP-системы:

- Пароли системных учетных записей (пользователем с правами администратора системы) должны изменяться ежеквартально;
- Каждый ответственный работник ИБ-отдела должен иметь персонифицированную учетную запись в DLP-системе;
- Все пароли системных учетных записей необходимо хранить в базе данных в зашифрованном виде, доступ к которой ограничен;
- Запрещается передача паролей пользователям при помощи почтовых сообщений либо иным другим открытым способом через Интернет.

4.2. Контроль за использованием технических средств в автоматическом режиме

4.2.1. Контроль за использованием технических средств в автоматическом режиме осуществляется на сетевом уровне передачи информации и на уровне технических средств, используемых работниками для выполнения их трудовых обязанностей.

4.2.2. На компьютеры пользователей устанавливается программное обеспечение DLP-системы, которое отслеживает всю активность, и передает данные администратору DLP-системы.

4.2.3. Контроль за использованием технических средств в автоматическом режиме включает в себя возможность фиксирования сведений о передаче работниками Компании защищаемой информации:

- по каналу электронной почты (корпоративной и личной[1] почты работника);
- на сторонние облачные хранилища (Яндекс.Диск, Dropbox и т.д.) и на внутренние сетевые ресурсы Компании;
- с помощью мессенджеров (Telegram, WhatsApp, Skype и т.д.);
- на ресурсы, расположенные в сети Интернет, с помощью интернет-браузера (Google Chrome, Mozilla Firefox и т.д.);
- на съемный носитель информации (флеш-накопители и мобильные устройства, подключенные к техническим средствам в режиме передачи файлов и т.д.).

4.2.4. Зафиксированные факты передачи / копирования защищаемой информации содержат в себе сведения о (об):

- отправителе информации (работнике Компании), включая IP-адрес технического средства;
- получателе(ях) информации (работнике Компании, контрагенте, конкуренте и ресурсе, на который передается защищаемая информация, и т.д.);
- времени и дате события;
- формате данных.

4.2.5. Контроль действий работников в автоматическом режиме осуществляется на постоянной основе.

4.3. Контроль за использованием технических средств в ручном режиме

4.3.1. В ручном режиме контроль осуществляется администратором DLP-системы, т.е. администратор имеет возможность в любой момент перехватить контроль за компьютером сотрудника.

4.3.2. Если за сотрудником было замечено нарушение, то с ним проводится профилактическая беседа.

4.3.3. Повторное действие того же сотрудника докладывается начальству, далее будут рассматриваться меры, которые будут приниматься в отношении этого сотрудника.

5. Ответственность

5.1. Ответственность за контроль выполнения мониторинга несут администраторы DLP- системы.

5.2. Контроль инцидентов осуществляется начальником ИБ.

5.3. Администраторы DLP-системы несут ответственность за обеспечение конфиденциальности и сохранности ПДн, доверенных им в рамках должностных обязанностей.

5.4. Компания обязуется не использовать программные (программно-аппаратные) средства контроля за использованием технических средств с целью умышленного тайного сбора личной информации работников Компании.

5.5. Ответственность за нарушение режима работы системы (рабочей станции, DLP системы) несут сотрудник рабочей станции и администратор DLP системы.

[1] В случае использования работником личной почты на техническом средстве, предоставленном Компанией для выполнения трудовых обязанностей.

6. Заключительные положения

6.1. Настоящее Положение является локально-нормативным актом Компании.

6.2. Актуализация настоящего Положения должна быть осуществлена в любом из следующих случаев:

- при изменении законодательства Российской Федерации в области защиты информации;
- по решению руководства Компании;
- при изменении целей / средств контроля использования технических средств;
- при изменении организационной структуры;
- при появлении необходимости в изменении процесса контроля использования технических средств.

6.3. Ознакомление работников Компании с требованиями настоящего Положения осуществляется работниками отдела информационных технологий, отдела информационной безопасности.

6.4. Контроль исполнения требований настоящего Положения осуществляется начальником отдела информационной безопасности.